3 DIGITAL MEDIA MODULE

3.1 Objectives

3.1.1 Understand and explain through oral demonstration the variety of digital media and their functions.

3.1.2 Understand and explain through oral demonstration the write blocker process.

3.1.3 Understand and explain through oral demonstration the process of imaging digital media.

3.1.4 Understand and explain through oral demonstration the function of the hash and its purpose.

3.1.5 Gain the capability to utilize various hardware and software programs utilized in the processing of digital media.

3.1.6 Gain the capability to perform wiping, imaging and hashing of digital media.

3.2 Methods of Instruction

3.2.1 Lectures

3.2.1.1 Removal of media.

3.2.1.2 Wiping digital media and its function.

3.2.1.3 Target drive preparation.

3.2.1.4 Hashing digital media and its function.

3.2.1.5 Imaging of digital media and its purpose

3.2.1.6 Removable media imaging

3.2.2 Literature Review

3.2.2.1 Kruse, Warren G. and Jay G. Heiser. Computer Forensic Response Essentials. Boston: Addison-Wesley, 2002.

3.2.2.2 Electronic Crime Scene Investigation: A Guide for First Responders. Washington, D.C.: U.S. Department of Justice, 2001.

3.2.2.3 Best Practices for Seizing Electronic Evidence A Pocket Guide for First Responders. 3rd ed. Washington, D.C.: U.S.

3.2.2.4 Digital Intelligence User's Manual.

3.2.2.5 Logicube Desktop Write Protect Hard Drive Imagers User's Manuals.

3.2.2.6 ILook User's Manual.

3.2.2.7 Owner's Manuals, User's Manuals and vender specific manuals should be referred to for equipment instructions.

3.2.2.8 Department of Forensic Science, Digital Evidence Procedures Manual – Sections 3 – 10.

3.2.2.9 Department of Forensic Science, Quality Manual.

3.2.2.10 New relevant material as it becomes available.

3.2.3 Training Programs

3.2.3.1 A+ Certification class or equivalent.

3.2.3.2 ILook Software training class or equivalent.

3.2.3.3 CyberCop Basic Data Recovery and Acquisition class or equivalent.

3.2.3.4 Additional computer forensic training (as approved by section supervisor)

3.2.3.5 General computer courses (as approved by section supervisor).

3.2.4 Demonstration

3.2.4.1 Related techniques will be observed from beginning to end and all notes will be generated by the trainee. These requirements will demonstrate that the trainee complied with all of the required procedures.

3.2.5 Laboratory Exercises

3.2.5.1 Digital Media Protection: Demonstrate the proper methods and techniques necessary to insure protection of various types of media.

3.2.5.2 Target Drive Preparation: Demonstrate the proper methods and techniques necessary to insure the target drive is properly prepared for use.

3.2.5.3 Hard Drive Imaging: Demonstrate the proper methods and techniques necessary to insure that the hard drive is imaged properly.

3.2.5.4 Removable Media Storage: Demonstrate the proper methods and techniques necessary to insure that the removable media is imaged properly.

3.3 Evaluation

3.3.1 Oral/ Written Examination

3.3.1.1 Oral review on each technique and procedure utilized in this section.

3.3.1.2 Written paper(s) on related topic to be assigned and approved by the section supervisor. This will be considered as a technical research paper.

3.3.1.3 Various techniques and terms to be defined both orally and written.

3.3.2 Laboratory Testing

- The trainee must complete at minimum of 1 year of casework under direct supervision of the Section Supervisor. This will include mock and actual cases demonstrating a variety of techniques and problem solving situations.

3.3.3 Oral Exercises

- Technical review sessions. The trainee MUST successfully complete this portion of the requirements.

3.3.4 Courtroom Exercises

- Trainee will be required to work a case that is representative of actual casework. Trainee must show the ability to defend the conclusions of the examinations and answer technical questions in a courtroom scenario. The trainee MUST successfully complete this portion of the requirements.

3.4 Examination Questions

3.4.1 Explain the process of digital media write protection and its purpose.

3.4.2 Explain a hash value and its purpose.

3.4.3 Explain target drive preparation and its purpose.

3.4.4 Explain the process of imaging digital media and its purpose.

3.4.5 Explain the process of imaging removable digital media.

3.4.6 Explain the following terms and techniques:

- Hard Drive
- Compression
- Encoding
- Hash Value
- Kilobyte, Megabyte, Gigabyte
- Wiping Process
- Motherboard
- Imaging
- File Extensions
- Proprietary File Formats
- Other terms and techniques may be added as necessary.

3.4.7 Define digital media protection.

3.4.8 Define target drive preparation.

3.4.9 Define hard drive imaging.

3.4.10 Explain the following:

- Bit Stream Copy
- MD-5 Hash

- Corrupt File
- File Extensions
- Compression
- Boot Disk
- Flash Card
- Thumb Drive
- SIM Card

3.4.11 Explain the most common limitations of processing digital media.

- Compression
- Time constraints
- File Volume
- System Files
- Proprietary Files

3.4.12 Explain the processes of wiping, imaging, hashing, examination, and reporting in a detailed manner.

♦End